Amendments To The Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing Of Claims

1. (Currently Amended) A packet based high bandwidth copy protection method comprising:

forming a number of data packets at a source device;

forming a first group of encrypted data packets by encrypting **some of** the data packets based upon a **first** set of encryption**/decryption** values**, wherein the number of encrypted data packets in the first group of encrypted data packets is less than the number of data packets formed at the source device**;

transmitting the encrypted **and unencrypted** data packets from the source device to a sink device coupled thereto;

decrypting the **first group of** encrypted data packets ~~based in part upon~~ using the **first set of** encryption**/decryption** values; and

accessing the decrypted **and unencrypted** data packets by the sink device.

2. (Original) A method as recited in claim 1, wherein the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets.

3. (Currently Amended) A method as recited in **claim 1** ~~claim 2~~, **further comprising:**

forming a first control data packet associated with the first set of encryption/decryption values; and

using the first control data packet to identify the first group of encrypted data packets, wherein the encryption/decryption **values** ~~**control signals**~~ include a Vsync, an Hsync, and a CNTL3.

4. (Currently Amended) A method as recited in claim 3, ~~**wherein each of the data packets is associated with an particular control packet**~~ **using the first set of encryption/decryption values included in the first control data packet to decrypt the first group of encrypted data packets**.

5. (Currently Amended) A method as recited in claim 4, wherein when the CNTL3 is active, then the corresponding data packet is encrypted ~~**and vice-versa**~~.

6. (Currently Amended) A system for providing high bandwidth copy protection in a packet based system, comprising:

a source unit arranged to provide a number of data packets;

a sink unit coupled to the source unit arranged to receive the data packets from thesource unit;

an encryption unit coupled to the source unit arranged to encrypt selected ones of the data packets sent from the source unit to the sink unit;

a decryption unit coupled to the sink unit arranged to decrypt the encrypted data packets; ~~**and**~~

an encryption/decryption values generator arranged to provide a set of encryption/decryption values **to the decryption unit that, in turn, uses the decryption values to** ~~**used**~~ ~~to encrypt and~~ decrypt ~~**the appropriate**~~ **any appropriately encrypted** data packets**; and**

processing the decrypted and unencrypted data packets by the sink unit.

7. (Currently Amended) A system as recited in claim 6, wherein ~~**the source unit is an audio/video unit arranged to provide audio type data packets and/or video type data packets**~~ **wherein the source unit is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets**.

8. (Original) A system as recited in claim 7, wherein the sink unit is a display unit arranged to display processed ones of the video data packets.

9. (Original) A system as recited in claim 8, wherein the display unit includes a number of speakers arranged to transmit audio signals based upon processed ones of the audio data packets.

10. (Original) A system as recited in claim 9, wherein the set of encryption/decryption control signals include Vsynch, Hsynch corresponding to the video data packets.

11. (Currently Amended) A system as recited in claim 10, wherein the set of encryption/decryption control **values** ~~**signal**~~ further includes CNTL3 to flag those data packets that are encrypted.

12. (Currently Amended) Computer program product **executable by a processor** for providing a packet based high bandwidth copy protection, **the computer program product** comprising:

computer code for forming a number of data packets at a source device;

computer code for encrypting **some of** the data packets based upon a set of encryption values**, wherein the number of encrypted data packets is less than the number of data packets formed at the source device**;

computer code for transmitting the encrypted data packets **and the unencrypted data packets** from the source device to a sink device coupled thereto;

computer code for decrypting the encrypted data packets based in part upon the encryption values;

computer code for ~~accessing~~ **processing** the decrypted data packets **and the unencrypted data packets** by the sink device; and

computer readable medium for storing the computer code.

13. (Original) Computer program product as recited in claim 12, wherein the source device is a video source and wherein the sink device is a video display and wherein the number of data packets include some audio data packets and some video data packets.

14. (Currently Amended) Computer program product as recited in claim 13, wherein the encryption control ~~signals~~ **values** include a Vsync, an Hsync, and a CNTL3.

15. (Original) Computer program product as recited in claim 14, wherein each of the data packets is associated with an particular control value CNTL3.

16. (Currently Amended) Computer program product as recited in claim 15, wherein when the CNTL3 is active, then the corresponding data packet is encrypted ~~and vice-versa~~.

New Claims

17. (New) A method as recited in claim 1, further comprising:

forming a second group of encrypted data packets by encrypting some of the number of data packets not already encrypted based upon a second set of encryption values; and

decrypting the second group of encrypted data packets using the second set of encryption values concurrently with the decrypting of the first set of encrypted data packets.

18. (New) A method as recited in claim 17, wherein the first set of encryption values is different than the second set of encryption values.

19. (New) A method as recited in claim 17 further comprising:

forming a second control data packet having encryption/decryption control signals associated with the second group of encryption values; and

using the second control data packet to identify the second group of encrypted data packets, wherein the encryption/decryption control signals include a Vsync, an Hsync, and a CNTL3 value.

20. (New) A method as recited in claim 3, using the encryption/decryption control signals included in the first control data packet to decrypt the first group of encrypted data packets.